PRIVACY POLICY

This Privacy Policy ("Privacy Policy") has been prepared by Sankalp Capital Private Limited ("Sankalp", "We", "our", "us"), a private limited company incorporated in India, having its registered office Office 112 Shakti Nagar, Kota, Rajasthan - 324005. Sankalp is a Non-Banking Financial Company ("NBFC") registered with the Reserve Bank of India ("RBI").

Sankalp provides the user ("You", "Your" or "User") accessing this website ("Website") or digital lending application, namely Upcash ("DLA"), operated by our lending service provider ("LSP") for availing the loan products offered by Sankalp Capital Private Limited (collectively, "Platform"). The purpose of this Privacy Policy is to give You information on how Sankalp collects, stores, uses, discloses, transfers and processes Your personal information when You use our Platform in order to avail our lending services ("Services").

You are advised to read this Privacy Policy along with the Terms and Conditions at https://sankalpcap.com and other information on the Platform ("Terms"). Users please take note that any statements made on Sankalp's Platform shall not be construed as an offer or promises for grant of any financial services or credit facilities to You.

This Privacy Policy has been prepared in compliance with:

- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- Reserve Bank of India (Non-Banking Financial Companies — Credit Facilities) Directions, 2025 ("Guidelines on Digital Lending");
- Digital Personal Data Protection Act, 2023 ("DPDPA") and corresponding rules, as may be notified from time to time.
- other applicable acts, regulations and rules which requires the publishing of a privacy policy for handling of or dealing in personal information including sensitive personal data or information and all applicable laws, regulations, guidelines provided by applicable regulatory authorities including but not limited to the RBI.

1. USER ACKNOWLEDGEMENT AND CONSENT

This Privacy Policy is incorporated into and at all times is subject to and is to be read in conjunction with the Terms.

You hereby expressly consent to provide the below mentioned information to Us for the purpose of providing the Services to You. If You disagree with any of the terms mentioned herein, please do not proceed with the usage of the Services.

For the Users consenting to continue accessing the Platform and availing the Services, this Privacy Policy explains our policies and practices regarding the collection, usage, and disclosure of Your information.

This Policy is an electronic record in the form of an electronic contract formed under applicable laws. This Policy does not require any physical, electronic, or digital signature. By accessing, browsing, using, or registering on our Platform, or by providing us with your personal data, you signify that you have read, understood, and agree to be bound by the terms of this Policy and consent to the processing of your

personal data as described herein. If you do not agree with the terms of this Policy, please do not access or use our Platform or Services.

2. PURPOSE OF COLLECTION

In general, you can browse the Platform without disclosing Your identity or revealing any personal information about Yourself. However, to create an account on the Platform, You will be required to provide us with certain personal information in connection with the Services. Our primary goal in accessing, collecting, processing and using Your information, is to provide You with a safe, efficient, smooth and customized experience of our Services.

3. WHAT WE COLLECT AND HOW WE USE YOUR PERSONAL DATA

The table below sets out (i) the personal data We collect or avail from third parties, (ii) the corresponding purpose of collection, (iii) the device permission (if any) through which We access the personal data, (iv) the frequency of such access, and (v) the Service use case for which the data set is collected/ to which the purpose is linked.

Personal Data	Purpose of Collection	Permission / Mode of Access	Frequency of Access
Name	Verification of User identity, and registering / onboarding the account on the Platform. Credit Underwriting KYC	Direct in-App entry by User	At onboarding/ during KYC
Date of birth	Age verification, (minors below 18 years are restricted from availing the Services); and identity verification; KYC	Direct in-App entry by User	At onboarding/ during KYC
Gender	Identity verification; KYC	Recorded during KYC	At onboarding/ during KYC
Employment status / occupation	Verification of financial credibility prior to sanction loan	Direct in-App entry by User	At loan application; on material change notified by User
Contact information (, email ID, mobile number)	Identity verification; KYC/ onboarding; verification of credit-worthiness; service communications including OTP-based authentication and communications relating to any loan availed or applied for	Direct in-App entry by User	At onboarding and on update by User/ KYC
Residential / correspondence address; Pincode	Determination of serviceability; KYC (Address verification) and identity / address verification	Direct in-App entry by User	At onboarding/ For KYC
PAN details, Aadhaar and other Government-issued identification documents (Officially Valid Documents)	Identity verification; and KYC; assessment of eligibility for the loan	Camera (one-time / on-demand) for loan and Storage / Files (read) where User uploads a soft copy	One-time or on-demand for each KYC session; not accessed in the background
Photograph/ Video (Video KYC)/ Camera/ Microphone	Scanning and capturing KYC documents, and conducting Video KYC	Camera	One-time or on-demand for each KYC or Video KYC session; not

Personal Data	Purpose of Collection	Permission / Mode of Access	Frequency of Access
			accessed in the background
Income details	Verification of credit-worthiness, and eligibility for the loan	Direct in-App entry by User; Storage / Files (read) where User uploads supporting documents	Loan application
Bank account details / UPI details	Verification of credit-worthiness and loan disbursement	Direct in-App entry by User; Storage / Files (read) where User uploads bank statements	At loan application and on update by User
NACH / e-mandate details	Repayment of amounts due under the loan	Direct in-App entry by User	At loan sanction; on each scheduled repayment cycle
Transactional SMS metadata (from 6-digit alphanumeric senders only)	Verification and analysis of financial position; determination of cash flow, credits, income and spending patterns to assess creditworthiness. Personal SMSs, OTPs (save where required solely to enable onboarding on the Platform) and account details are not read or stored.	SMS (read) — collected only with the User's explicit prior consent and with audit trail in accordance with the Guidelines on Digital Lending	Collected only during loan application and underwriting; not accessed in the background after underwriting is complete
Device GPS location	For KYC/ onboarding and location verification. Reducing fraud risk associated with loan applications, and determining serviceability of a loan application based on location	Location	Accessed at the time of onboarding and loan application; not accessed continuously in the background
User-uploaded documents (bank statements, identity documents, income proofs)	Uploading KYC and financial documents required for loan application processing, and	Storage / Files (read)	Accessed only when the User actively selects and uploads a file; not accessed in the background
Address Proof (utility bills / passport / driving license / voter id)	Verification of credit-worthiness and loan disbursement	Direct in-App entry by User	At onboarding/ For KYC
Device data (IP address, browser type and version, time-zone, operating system, device information)	Data analytics; fraud prevention; security monitoring and incident detection.	Captured server-side at session level	On each session; not accessed in the background
Marketing and communications preferences	Recording the User's preferences regarding marketing communications and communications under DND / NCPR settings	Direct in-App entry by User	At onboarding and on update by User

Personal Data	Purpose of Collection	Permission / Mode of Access	Frequency of Access
Credit Reports	For credit underwriting	Direct in-App entry by User	At onboarding and on update by User/ during KYC

"Information We collect about You from third parties": This type of data is personal data about You received from various third parties and public sources including our third-party service providers for advertising and User analytics purposes, and other publicly available sources in connection with our provision of Services to You, or in connection with Your use of the Platform or Services that You choose to avail. For making the Services available to You, We may collect credit information in accordance with applicable laws, from certain third parties such as credit bureaus or credit rating companies, account aggregators, financial institutions from time to time during the loan journey. In order to provide credit products to You, We may receive certain information pertaining to document verification, repayment status etc. from certain third parties including UIDAI, Digilocker, NSDL or other PAN databases, credit bureaus, payment gateway providers. We may further collect Your bank account numbers or UPI payment information for collection and repayment of loans.

How We use this information: We shall collect and use this information on a need basis for the provision of Services and for performing due diligence and verification of Your loan application. Please note that we do not have any control over personal data that You may choose to make publicly available. For example, if You post reviews, comments, or messages on public sections of the Platform or on an application store (such as the Play Store), You do so at Your own risk. We are not liable for any third-party misuse of such data.

4. STORAGE OF INFORMATION

We store Your information in the servers located within India.

We ensure that no biometric data belonging to You shall be collected by our DLA or stored by our LSP through DLAs. In case, if any of our representatives ask for the same from You, We request You to kindly refrain from doing the same and address this concern to our Grievance Officer (the details of the same have been provided below in Clause 12).

We retain any data or information provided by You for the period mandated under applicable law. Our data retention policy is restricted to our provision of Services.

In the event of a data breach, We act swiftly to contain and investigate the incident. We report incidents to CERT-IN within 6 (six) hours of discovery and notify regulatory bodies, impacted customers, and other relevant parties as required. Corrective actions are taken to strengthen security, and We provide support to affected customers as necessary.

5. DATA RETENTION GUIDELINES

Category of Personal Data	Purpose of Processing	Retention Period
Identity and KYC Data (Full name, PAN, Aadhaar, date of birth, address)	Your Identification; satisfaction of KYC obligations mandated by the Reserve Bank of India	5 years from the date of loan closure, or as prescribed under applicable law, whichever is the later

Category of Personal Data	Purpose of Processing	Retention Period
Financial Information (Bank statements, salary slips, income documentation)	Assessment of creditworthiness and determination of eligibility for loan products	5 years from the date of loan closure
Loan Account Records (Disbursement details, repayment history, EMI schedules)	Administration of the loan account; mandatory reporting to credit information companies	5 years from the date of loan closure
Credit Information (Credit scores and bureau reports)	Evaluation of credit risk prior to sanction of a loan facility	6 months from the date of consent
Bank Account and Payment Details (Account number, UPI ID)	Disbursement of loan proceeds; collection of scheduled repayments	Duration of loan tenure plus 5 years
Device and Network Information (Device ID, IP address)	Fraud detection and prevention of unauthorized access to Your accounts	180 days from the date of collection
SMS and Transaction Data (transactional SMS, transaction history on Platform) (from 6-digit alphanumeric senders only)	Assessment of financial position; cash flow analysis; creditworthiness evaluation	1 day from the date of collection
Communication Records (Email correspondence, call recordings, chat transcripts)	Dispute resolution; satisfaction of regulatory audit requirements	5 years from the date of the relevant interaction
Consent Audit Trail (record of consents granted, denied or withdrawn by the You at each stage of the loan journey, including the nature of consent, timestamp and channel)	Regulatory compliance; evidence of lawful basis for processing at each stage; audit and inspection requirements under RBI's Guidelines on Digital Lending	1 year from the date of full repayment or account closure, whichever is the later
Applications that are rejected or not proceeded with	Regulatory compliance; dispute resolution	5 years from the date of rejection or last activity

Personal data shall not be retained beyond the applicable retention period, except where:

- Retention is required for the resolution of an ongoing dispute or legal proceeding;
- A competent regulatory authority has directed retention of the data; or
- The Customer has not yet repaid the loan in full, in which case such data as is necessary for the administration of the outstanding facility shall be retained until repayment is completed.

Anonymized Data: Personal data that has been irreversibly anonymized, such that it can no longer be used to identify any individual, ceases to constitute personal data for regulatory purposes. We may retain anonymised or aggregated datasets for internal analytics and statistical purposes following the expiry of the applicable retention period.

6. DATA DELETION AND DESTRUCTION PROTOCOL

Upon expiry of the applicable retention period for each category of personal data, We follow the structured destruction process set out below:

1. **Digital data:** Digital data stored on Our servers shall be permanently and irreversibly deleted using industry-standard secure deletion processes.

2. **Physical documents:** Where physical documents containing personal data have been generated, such documents shall be destroyed by certified shredding through an authorized disposal vendor.
3. **Backup copies:** Backup copies of personal data shall be purged within the scheduled backup rotation cycle following the expiry of the retention period.
4. **Destruction log:** A destruction log shall be maintained as a permanent compliance record and shall not itself be subject to destruction. At minimum, the log shall record: the category of data destroyed, the volume or identifiers of records destroyed, the method of destruction employed, the date of destruction, and the name and designation of the authorized personnel who certified the destruction.
5. **Suspension of destruction:** In the event of any litigation, regulatory investigation, dispute or other proceeding that is ongoing or reasonably foreseeable (each, a "Suspension Event"), destruction of all records that are or may be relevant to such Suspension Event shall be immediately suspended. Scheduled purges shall not proceed in respect of such records until the Suspension Event has been fully resolved and Our legal function has confirmed in writing that destruction may resume.

Right to request deletion: You may request the deletion of Your personal data by writing to us at support@sankapcap.com. We will process such request subject to the following conditions:

- any loan facility availed by You must be fully repaid before deletion of loan account data can be processed;
- We shall retain such data as is required under applicable laws, including the Prevention of Money Laundering Act, 2002 and RBI guidelines, for the statutory minimum period, regardless of a deletion request; and
- We shall communicate to You the categories of data that cannot be deleted and the reason therefor within 30 days of receipt of such request.

7. USE OF INFORMATION COLLECTED BY SANKALP

The information collected from You will be used by Sankalp for the following purposes:

- To provide Services You have requested;
- To establish identity, conduct KYC and verify the same in compliance with the applicable laws;
- To resolve disputes and help investigate violations of our Terms or to defend against legal claims;
- To disclose the information under special circumstances such as compliance with the applicable local law, court summons, court orders, requests/order from legal authorities or law enforcement agencies requiring such disclosure;
- To assess Your creditworthiness for providing the Services;
- To get in touch with You (either directly or through our partners, agents, or LSPs) when necessary and contact You by email, SMS, letter, WhatsApp, telephone or in any other way about our products and Services, including for any transaction, promotion activity, marketing and/or commercial communications in relation thereto.
- To identify, prevent, detect or tackle fraud, money laundering, terrorism and other crimes;
- To identify, develop or improve products, that may be of interest to You;
- To perform other administrative and operational purposes including the testing of systems;
- To recover any payments You owe to us or to our partners;

- To undertake filing of records with the relevant government / Statutory authorities in compliance with the applicable laws;
- Comply with our regulatory and legal obligations;
- To maintain records under applicable law or a may apply to pursuant to agreements executed by Sankalp;
- To carry out, monitor and analyze our business, carry out audits, market research, business, and statistical analysis and also direct our efforts for product improvement; and
- We collect all data and other necessary information under this Privacy Policy or otherwise on a need basis required for the above intended purposes in compliance with applicable laws.

8. DISCLOSURE OF INFORMATION

We will share Your information that We collect (except for any device information) only in such manner as described below and limited to the extent required for providing the Services (including through partners of Sankalp):

- We disclose and share Your information with our LSPs, partner banks, data processors, financial institutions, credit bureaus and other third-party partners (such as Direct Sales Agents ("DSA") and Debt Recovery Agents ("DRAs")) for facilitation and recovery pertaining to loan or facility or line of credit or purchase of a product.
- To enable our third-party partners to contact You or to respond to Your queries / comments, for promotional offers or to resolve service issues to serve You better.
- We will disclose the data or information provided with other technology partners to track how You interact with the Platform on our behalf.
- We and our affiliates may share Your information with other business entity should We (or our assets) merge with, or be acquired by that business entity, or re-organization, amalgamation, restricting of business for continuity of business. Should such transaction occur than any business entity receiving any such information from us shall be bound by this Privacy Policy with respect to Your information.
- We may share Your personal information upon receipt of notice/communication/ order, as a part of our legal obligations and as per applicable laws with the government /quasi government authorities, judicial / quasi-judicial authorities.

By using our Services, You hereby provide Your consent to disclose Your personal information for the above-mentioned purposes. Any disclosure to third parties is subject to the following:

- If We are under a duty to disclose or share Your personal data in order to comply with any legal or regulatory obligation or request, We shall not seek Your explicit consent however We shall reasonably endeavor to notify the same to You accordingly as the case may be;
- We shall take Your express consent in the event We share Your personal data with third parties;
- We shall share Your information with third-party only on a need basis and only for the purpose stated hereunder, as per the applicable laws.
- We shall additionally seek express consent through a specific consent for at appropriate stages of data collection, if required under applicable laws.

Usage of Your information by such third parties is subject to their privacy policies. We share information to the extent required. We also suggest You go through the privacy policies of such third parties.

The list of our lending service providers and digital lending applications of our lending service providers (as amended from time to time) are accessible on our Website at https://www.sankalpcap.com.

Third parties with whom we may share Your data for providing Services are detailed on the Company website available at https://www.sanakapcap.com/

9. INFORMATION SECURITY

Sankalp intends to protect Your information and to maintain its accuracy as confirmed by You. We implement reasonable physical, administrative and technical safeguards to help us protect Your information from unauthorized access, use and disclosure. For example, We encrypt all information when We transmit the data in digital form. We also require that our registered third-party service providers protect such information from unauthorized access, use and disclosure.

Sankalp has adequate security measures in place to protect the loss, misuse and alteration of information under control. We endeavor to safeguard and ensure the security of the information provided by You. We use Secure Sockets Layers (SSL) based encryption, for the transmission of the information, which is currently the required level of encryption in India as per applicable laws.

We blend security at multiple steps within our products with state-of-the-art technology to ensure our systems maintain strong security measures and the overall data and privacy security design allow us to defend our systems ranging from low hanging issue up to sophisticated attacks.

We protect personal data by taking reasonable security safeguards to prevent personal data breach, which shall include, at the minimum:

- appropriate data security measures, including securing of such personal data through its encryption, obfuscation or masking or the use of virtual tokens mapped to that personal data;
- appropriate measures to control access to the computer resources;
- visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorised access, its investigation and remediation to prevent recurrence;
- reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, including by way of data backups;
- for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise;
- appropriate technical and organisational measures to ensure effective observance of security safeguards.

We aim to protect from unauthorized access, alteration, disclosure or destruction of information We hold, including:

- Encryption of data to keep Your data private while in transit;
- Security feature like an OTP verification to help You protect Your account;
- Review our process of collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems;
- Restricted access to personal information to our staff, representatives, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict

contractual confidentiality obligations and suitable disciplinary action taken, in case if they fail to meet these obligations;

- Compliance & cooperation with regulations and applicable laws;
- Periodic review of this Privacy Policy and make sure that We process Your information in ways that comply with it.
- Non-disclosure of Aadhaar number in any manner. We comply with legal frameworks relating to the transfer of data as mentioned and required under the Information Technology Act, 2000, rules and the amendments made thereunder.
- On receipt of formal/ written complaints, We respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of Your data that We cannot resolve with You directly.

10. COOKIES

The Platform uses temporary cookies to store certain data that is used by us for maintenance of the Platform and its features as well as for research and development. We do not store personal/identity information in the cookies.

The cookies shall not provide access to data in Your device such as email addresses or any other data that can be traced to You personally. The data collected by way of cookies will allow the Platform to provide more enhanced and personal features, enabling delivery of more User-friendly services.

Most devices allow You to configure settings to notify You when a cookie is received or to block cookies altogether. However, disabling cookies may restrict the functionality and features available on the Platform or limit access to certain Services. Additionally, some pages on the Platform may include cookies or similar technologies implemented by third parties. Please note that We do not control the use of cookies by these third parties.

11. THIRD PARTY SDKS AND OTHER SITES

The Platform has a link to registered third party software development kits (“SDKs”), Application Programming Interface (“API”) integrations, redirections which collects data on our behalf and data is stored to a secured server. We ensure that our third-party service providers take extensive security measures in order to protect Your personal information against loss, misuse or alteration of the data as required under the applicable laws.

However, We are not responsible for the privacy practices or the content of those linked websites. With this Privacy Policy, We are only addressing the disclosure and use of data collected by Us. Their data collection practices, and their policies might be different from this Privacy Policy and We do not have control over any of their policies neither do We have any liability in this regard.

Our third-party service providers employ separation of environment and segregation of duties and have strict role-based access control on a documented, authorized, need-to-use / know basis. The stored data is protected and stored by application-level encryption. They enforce key management services to limit access to data.

Furthermore, our registered third-party service providers provide hosting security – they use industry leading anti-virus, anti-malware, intrusion prevention and detection systems, file integrity monitoring, and application control solutions.

We don't allow unauthorized access to Your non-public personal contacts or financial transaction SMS data by any third party in relation to Services other than our authorized partners for the Services.

12. DND / COMMUNICATION OPT-OUT

Once You register on the Platform and sign in, You are not anonymous to the Company. In the event Your account is created using Your cell phone number and password, email address and password, or social media logins (as applicable), You authorize us (including its business partners) to send texts and email alerts to You with Your login details and any other service requirements, including promotional communications, even if You have registered yourself under DND or DNC or NCPR services. Your authorization shall be valid as long as Your account is not deactivated.

You confirm that laws concerning unsolicited communication referred to in the "National Consumer Preference Register" (NCPR Registry) will not be applicable for communications received from us in connection with Your loan application for Credit Facility and the Services.

13. YOUR RIGHTS

Modifying or rectifying Your information: You are responsible for providing us with accurate and complete personal data. In the event of any personal information provided by You is inaccurate, incomplete or outdated then You shall have the right to provide Us with the accurate, complete and up to date data and have us rectify such data at our end immediately.

We urge You to ensure that You always provide us with accurate and correct information/data to ensure Your use of our Services is uninterrupted. In case of modification of personal information, You will be required to furnish supporting documents relating to change in personal information for the purpose of verification by Sankalp.

Your Privacy Controls: You have certain choices regarding the information We collect and how it is used:

- Your device may have controls that determine what information We collect. For example, You can modify permissions on Your android/iOS device or browser to remove any permissions that may have been given. However, Sankalp does not provide a guarantee of Services if any such controls are exercised / access is denied.
- You can also request to remove content from our servers in accordance with sub-clause (iii) below.

Withdrawal/Denial of consent: You acknowledge that We have duly collected the information with Your consent and You have the option to not to provide such information, or deny consent for use of specific information, restrict disclosure by us to any third parties, deny retention by us of any of Your information, or revoke the consent already given for any of the above, and if required, make the /our DLAs delete/forget any such information. However, any withdrawal of such personal information will not be permitted in case any Service availed by You is active and such information is necessary to be retained by us or DLA/LSP/third party partners until the continuation of Services, or until such duration as stipulated under any applicable laws, whichever is later. Where consent has been withdrawn by you, We do not guarantee and cannot be liable for providing such Service. For exercising your right to withdraw/deny consent as per this clause, please contact us at support@sankalpcap.com.

You shall have the following rights pertaining to Your information collected by us:

- **Deny Consent:** You shall have the right to deny consent for use of specific data, restrict disclosure of your data to third parties, revoke consent already granted to collect personal data, opt for preferences as to data retention, and if required, make the Platform delete/ forget the data. However, any such denial will not prejudice our right to retain any data in relation to the loans or

credit facilities availed by You. Further, in case of a denial of consent, the Platform does not provide a guarantee or will not be liable towards the continued facilitation of the Services if any such controls are exercised.

- **Withdraw Consent:** You may withdraw Your consent to contact You, for the continued collection, use or disclosure of Your information, at any time, or request for deletion of Your login account to the Platform by raising a request on the Platform or by mailing us at support@sankalpcap.com. However, We do not provide guarantee of continued provision of Services if any such controls are exercised / access is denied. Further, in the event the request for withdrawal is made while any credit facility or loan taken by you is outstanding, We shall have the right to continue processing Your information till such credit facility has been repaid in full, along with any interest and dues payable and/or for such period as may be allowed under applicable law. However, We shall not retain Your data and information if it is no longer required by us and there is no legal requirement to retain the same, and such data will be destroyed/purged in line with our internal policies. Do note that multiple legal bases may exist in parallel, and We may still have to retain certain data and information at any time to comply with applicable laws. Also, the information may still be used for execution of any outstanding or termination activity of any Services.
- **Report an issue:** You have the right to report any security breach / incident to the Grievance Redressal Officer (GRO) of Sankalp (details mentioned hereinbelow). You are entitled / shall be entitled to prevent unauthorized usage of Your information by our personnel/staff / representative / agents by informing us immediately / within 10 days of being informed of the proposed use, that You do not wish to disclose such information. You can also exercise the right at any time by contacting us at support@sankalpcap.com
- Information/data deletion may not be implemented for ongoing Services including loan, insurance policy (if any).
- **Marketing and Communication:** The consent for this information can be withdrawn by sending an email to support@sankapcap.com

14. YOUR DUTIES AS THE USER

You are required to:

- Not impersonate another person while providing your personal data for any specified purpose;
- Not suppress any material information while providing your personal data for any purpose;
- Provide only such information as is true, necessary, and verifiable for the purpose for which it is provided.

15. PROHIBITED ACTIONS

While visiting or using the Platform, You agree not to, by any means (including hacking, cracking or defacing any portion of the Platform) indulge in illegal or unauthorized activities including the following:

- Restrict or inhibit any authorized user from using the Platform.
- Use the Platform for unlawful purposes.
- Harvest or collect information about Platform's users without their express consent.
- "Frame" or "mirror" any part of the Platform without our prior authorization.
- Engage in spamming or flooding.

- Transmit any software or other materials that contain any virus, time bomb, or other harmful or disruptive component.
- Remove any copyright, trademark or other proprietary rights notices contained in the digital platform.
- Use any device, application or process to retrieve, index, “data mine” or in any way reproduce or circumvent the navigational structure or presentation of the digital platform.
- Permit or help anyone without access to the digital platform to use the digital platform through Your username and password or otherwise.

16. CHANGES IN PRIVACY POLICY

Our Privacy Policy might change from time to time, and Sankalp will provide notice of it on Your email address linked to Your Platform account or can be seen by You in our Platform. We encourage You to periodically review the Platform for the latest information on our privacy practices. Users are bound by any changes to the Privacy Policy hosted / made available on the Platform.

17. GRIEVANCE REDRESSAL AND FURTHER INFORMATION

In case You have any grievance relating to collecting receiving, possessing, storing, dealing or handling of Your personal information provided, You may refer the Grievance Redressal Mechanism available at support@sankalpcap.com/policies/grievance-redressal.